ABSTRACT OF THE DISCLOSURE

An encryption apparatus performs high-speed and secure signature creation and verification. In the encryption apparatus, at least a shift register group composed of shift registers for retaining values for arithmetic operations for generating a hash value for use in public-key-cryptosystem encryption processing, and shift registers for capturing a resultant hash value, and a shift register group composed of shift registers for retaining values for arithmetic operations for performing public-key-cryptosystem encryption processing and shift registers for capturing an arithmetic result are used for each other. Hardware components to be operated are changed in a time-sharing manner in accordance with a processing mode.